PCT/IB 0 4 / 0 0 6 1 2
02. 03. 04

SCHWEIZERISCHE EIDGENOSSENSCHAFT
CONFÉDÉRATION SUISSE
CONFEDERAZIONE SVIZZERA

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

Bescheinigung

Die beiliegenden Akten stimmen mit den ursprünglichen technischen Unterlagen des auf der nächsten Seite bezeichneten Patentgesuches für die Schweiz und Liechtenstein überein. Die Schweiz und das Fürstentum Liechtenstein bilden ein einheitliches Schutzgebiet. Der Schutz kann deshalb nur für beide Länder gemeinsam beantragt werden.

Attestation

Les documents ci-joints sont conformes aux pièces techniques originales de la demande de brevet pour la Suisse et le Liechtenstein spécifiée à la page suivante. La Suisse et la Principauté de Liechtenstein constituent un territoire unitaire de protection. La protection ne peut donc être revendiquée que pour l'ensemble des deux Etats.

Attestazione

I documenti allegati sono conformi agli atti tecnici originali della domanda di brevetto per la Svizzera e il Liechtenstein specificata nella pagina seguente. La Svizzera e il Principato di Liechtenstein formano un unico territorio di protezione. La protezione può dunque essere rivendicata solamente per l'insieme dei due Stati.

Bern, 19. FEB. 2004

Eidgenössisches Institut für Geistiges Eigentum
Institut Fédéral de la Propriété Intellectuelle
Istituto Federale della Proprietà Intellettuale

Patentverfahren
Administration des brevets
Amministrazione dei brevetti

H. Jenni

Heinz Jenni

Proprietà Intellectual

Hinterlegungsbescheinigung zum Patentgesuch Nr. 01544/03 (Art. 46 Abs. 5 PatV)

Das Eidgenössische Institut für Geistiges Eigentum bescheinigt den Eingang des unten näher bezeichneten schweizerischen Patentgesuches.

Titel:
Duales - Netzwerk.

Patentbewerber:
Csaba Bona
Laufenburgerstrasse 5
4310 Rheinfelden

Anmeldedatum: 10.09.2003

Voraussichtliche Klassen: G06F, H04L

Unveränderliches Exemplar
Exemplaire invariable
Esemplare immutabile

Beschreibung

Duales – Netzwerk
Internet Sicherheit

1. Stand der Technik.

1.1 Datenkommunikation heute.

Die Daten werden **seriell** in Pakete aufgeteilt. Das heisst folgendes: die ersten X – Bytes (Bits) werden als Paket 1, die zweiten X – Bytes (Bits) werden als Paket 2, u.s.w definiert. Diese Pakete werden dann in einem Netzwerk (z.B. im Internet) vom Absender zum Empfänger gesendet. Die Pakete enthalten – ausser Daten - Adressen und Regeln, wie sie beim Empfänger wieder zusammengesetzt werden müssen. Auch wenn zum Teil verschlüsselt, ist **alles am selben Ort, zum selben Zeitpunkt (Zeitfenster), in einem Paket und im selben Netzwerk** zu finden. Gerade deshalb sind die Daten in solchen Paketen in **einem** Netzwerk für den unbefugten Zugriff so anfällig.

2. Detaillierte Darstellung der Erfindung.

Das Ziel des Verfahrens ist es den unbefugten Zugriff auf vertrauliche Daten und das unbefugte Eindringen in Computer – Systeme (durch Hacker) zu vereiteln. Zumindest die heute bekannten Raten von Hacker – Attacken (vor allem, aber nicht ausschliesslich über das Internet) drastisch zu reduzieren.

2.1 Die neue Paket – Erstellung für das Duale - Netzwerk.

Das Verfahren beginnt mit der neuen Methode der Paketerstellung. Aufteilung der Information in U – Pakete und in G – Pakete.

BIT Nummer	0	1	2	3	4	5	6	7	8	9	10	N	Paket Länge*
Paket heute	1	1	0	0	1	0	0	1	1	1	0	...	4096
U – Paket*		1		0		0		1		1		...	2048
G – Paket*	1		0		1		0		1		0	...	2048

*) U – Paket = ungerade BITs, G – Paket = gerade BITs, die Paket Längen sind nur Beispiele

Tabelle 1

Es sind 2048 BITs/Paket/Netzwerk (U – Netzwerk und G – Netzwerk). Weit über der kritischen Länge pro U - Paket und pro G – Paket. Die heutigen Computer können diese Länge der Pakete nicht – innerhalb nützlicher Frist – kombinatorisch errechnen. (Alle Möglichkeiten "ausprobieren", durch ein Computer – Programm.)

Merken wir die neue Art der Aufteilung der Daten (Information) in U – und in G – Pakete, die zwei, für sich nutzlose, Hälfte der Information erzeugt. Diese Art der Aufteilung "verbirgt" auch die implizite Verschlüsselung der Daten. Wie ein in zwei Stücke gebrochenes Amulett, deren Zusammengehörigkeit der Betrachter (nur der Empfänger) erst beim Zusammenlegen der zwei Hälften erfährt. Wir merken auch, dass die implizite Verschlüsselung ein Ersparnis an Bandbreite oder eine Erhöhung des Durchsatzes bewirkt.

2.2 Datenkommunikation im Dualen - Netzwerk.

2.2.1 Was ist das Duale – Netzwerk nicht?

Diese Techniken können im Dualen – Netzwerk verwendet werden, aber sie sind nicht das Duale – Netzwerk.

- Kein virtuelles Netzwerk.
- Keine mehrfache Mail - Adressen pro Benutzer. (Z.B: x.yyy@smile.ch und y.xxx@teleport.ch)
- Keine mehrfach Verbindung um die Bandbreite über mehreren Kanälen auszunutzen.
- Auch keine mehrfach vergebene IP – Adressen.

- Kein Multi – Pfad – Routing.
- Kein IPv4 oder IPv6 Netzwerk (Protokoll),
mit mehreren privaten IP – Adressen für eine öffentliche (public) IP – Adresse.

2.2.2 Was ist das Duale – Netzwerk?

Hier handelt es sich effektiv um zwei, klar getrennte Netzwerke, ohne gemeinsamen Knoten. Also eine Quasi - Verdopplung des gesamten Internets, Intranets, LANs, etc...Nennen wir sie: U – Netzwerk und G – Netzwerk. (U = ungerade, G = gerade).
Unter Verdopplung, ist die Verdopplung der Anzahl der Knoten - im heutigen Netzwerk - zu verstehen: U – Knoten, G – Knoten (Nicht am selben Ort!! Siehe Abbildung 1)

Nur Quasi – Verdopplung, weil die Anzahl der U – Knoten und die Anzahl der G – Knoten nicht identisch sein müssen. (Die Anzahl Router oder Gateway, im U – Netzwerk und im G – Netzwerk müssen nicht identisch sein.)

Jedes End - Gerät (PC, Server, etc.) verfügt über zwei Identitäten: U – Identität, G – Identität. Die Benutzer hingegen behalten ihre einmalige Identität. Sie benutzen nur End - Geräte, welche über zwei Identitäten verfügen. Die eine verbindet es mit dem U – Netzwerk, die andere mit dem G – Netzwerk. Die U – Pakete suchen ihren Weg im U – Netzwerk, die G – Pakete im G – Netzwerk. Ohne Hinweis darauf, dass sie zusammengehören und dass sie dasselbe End - Gerät erreichen werden. Die räumliche (geografische) und die spektrale Trennung der Daten während der Übertragung geben dem unbefugten Zugriff zu den eigentlichen Daten so gut wie keine Chance.

Geräte, die für das weiterleiten der Pakete im jeweiligen Netzwerk zuständig sind (Router, Gateway, etc.), sind jeweils nur an ein Netzwerk angeschlossen (U – Netzwerk oder G – Netzwerk) und erfüllen ihre Aufgaben, als ob es nur ein Netzwerk gäbe. Wie es (heute) vor der Einführung des Dualen – Netzwerkes üblich ist.

Für die zwei Netzwerke, wird keine Grenze der Spektrum – Aufteilung definiert. Das zur Verfügung stehende Spektrum (Bandbreite) wird durch die beiden Netzwerke dynamisch genutzt. Diese dynamische Zuordnung der Kanäle und das dynamische Routing verschafft die räumliche (geografische) und die spektrale Trennung der U – und der G – Pakete während der Übertragung.

Nun – beim Empfänger, nach der Übertragung – werden die zwei Hälften (U – Paket, G – Paket) des Amuletts aneinandergelegt. Passen sie zusammen?

Eine Sendung (Mail, oder auch eine Web – Seite) besteht meistens aus mehr als nur einem Paket. Ein Bestandteil der Pakete ist eine Identifikation der Sendung (Message – ID). Im Dualen - Netzwerk, eine für das U – Netzwerk und eine für das G – Netzwerk. Am Ende der Übertragung – als letztes U - Paket - sendet der Absender die G - Message – ID der Sendung im G – Netzwerk (oder umgekehrt) an den Empfänger. So ist der (berechtigte) Empfänger in der Lage die U – und G – Pakete wieder zusammenzusetzen. [Siehe Abbildung 1 (Duales - Netzwerk)]

Theoretisch kann das Duale – Netzwerk als N – Netzwerk verallgemeinert werden.

2.3 Beschreibung der Message - ID.

Das Verfahren endet mit dem Zusammenführen der U – Pakete und der G – Pakete, um an die vermittelten Daten heranzukommen.

Die Message – ID stellt eine Möglichkeit dar, die U – Pakete und die G – Pakete, beim Empfänger, zusammenzuführen. Nach Zufall verschlüsselte Bit – Sequenz. U – Message – ID, für das U – Netzwerk, G – Message – ID, für das G – Netzwerk. Das letzte U – Paket liefert beide Message – IDs:
U – Message – ID und G – Message – ID.

Sollte eine U - Message – ID oder eine G - Message – ID, zu einem bestimmten Zeitpunkt beim Empfänger mehrfach vorkommen, so müssen die betroffenen Sendungen wiederholt werden.

2.4 Kabel, Glasfaser oder Luft (drahtlos).

Das hier vorgeschlagene Duale – Netzwerk ist für beliebiges Übertragungs – Medium geeignet. Zweifellos ist das Anschliessen der End – Geräte an die zwei Netzwerke im Falle der drahtlosen Kommunikation einfacher.

2.5 Zertifizierung, Signatur, Kryptographie.

Herkömmliche Zertifizierung, Signatur, Kryptographie, etc. können in Kombination mit dem Dualen – Netzwerk eingesetzt werden.

Patentansprüche

1. Patentansprüche.

Beinhaltet zwei zusammenhängende Elemente:

1. Duales – Netzwerk (Siehe 1.1 Duales – Netzwerk)

2. Neue Methode der Paket – Erstellung (Siehe 1.2 Neue Methode der Paket – Erstellung)

U – Pakete "bewegen" sich ausschliesslich im U – Netzwerk.
G – Pakete "bewegen" sich ausschliesslich im G – Netzwerk.

1.1 Duales - Netzwerk.

Zwei Identitäten (Knoten) der beteiligten End - Geräte: U – Identität und G - Identität
Räumliche (geografische) und spektrale Trennung der zusammengehörenden U – und G – Pakete, während der Übertragung. (Siehe Zeichnung, Abbildung 1)

1.2 Neue Methode der Paket - Erstellung.

Jedes zweite Bit wird in ein Paket zusammengefasst: U – Paket und G – Paket.
(Siehe Beschreibung, Tabelle 1)

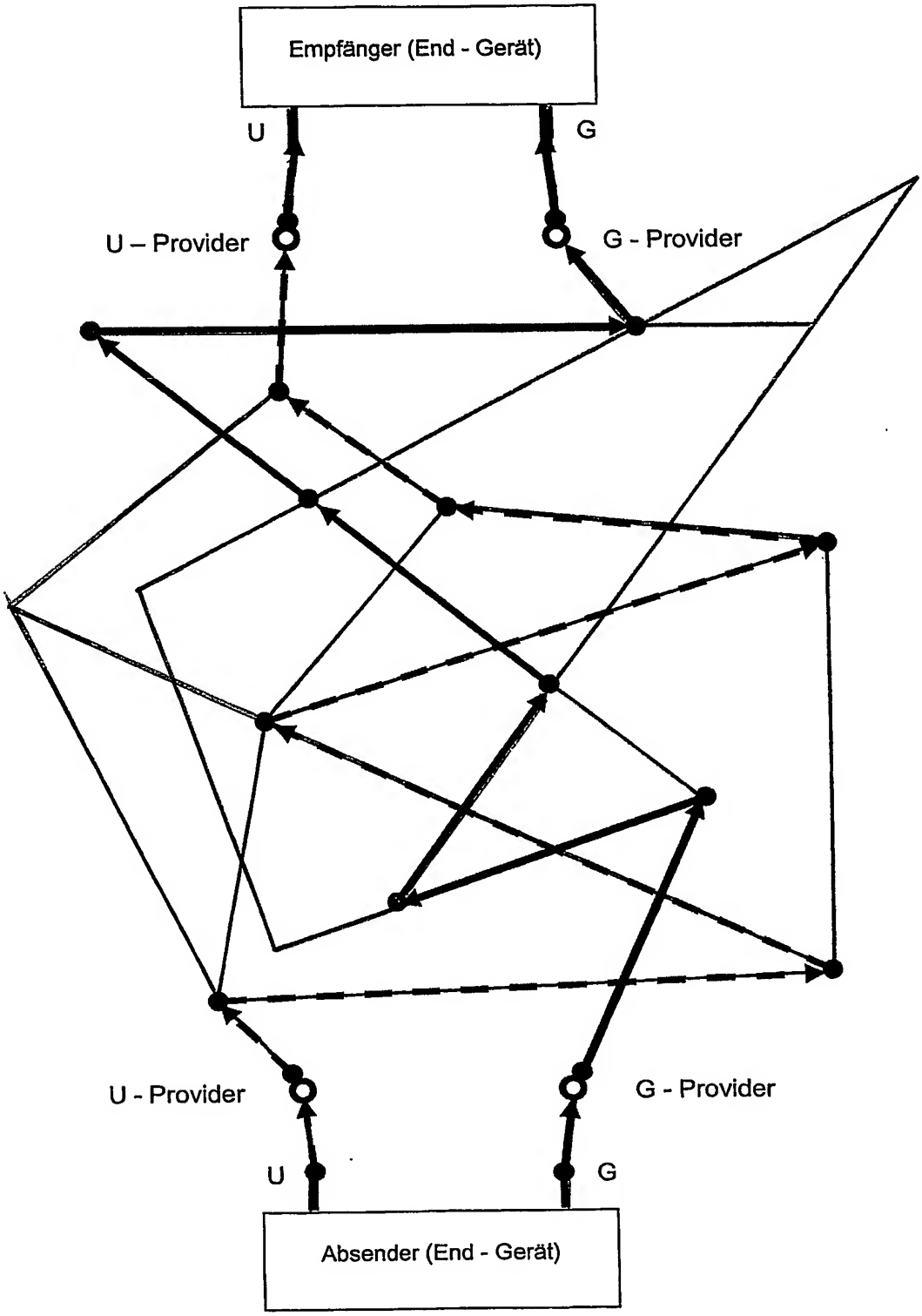
Zusammenfassung

Internet – Sicherheit durch Duales – Netzwerk (zwei Netzwerke) und durch eine neue Methode der Paket – Aufbereitung. Wie ein in zwei Stücke gebrochenes Amulett (Pakete), deren Zusammengehörigkeit der Betrachter (nur der Empfänger) erst beim Zusammenlegen der zwei Hälften erfährt.

Die zwei Stücke (Pakete) beschreiten getrennte Wege (in getrennten Netzwerken) beim Absender, verraten ihr Geheimnis (ihre Zusammengehörigkeit) erst, nach der Übertragung der gesamten Information, beim Empfänger.

Zeichnung

Duales - Netzwerk



U = ungerade, G = gerade, ⟶ = U – Paket (im U – Netzwerk), → = G – Paket (im G – Netzwerk)

Abbildung 1